EXPRESS MAIL CERTIFICATE

Date: May 7, 1999 Label No. EL284834038US
I hereby certify that, on the date indicated above I deposited this paper or fee with the U.S. Postal Service and that it was addressed for delivery to Box Patent Application, the Assistant Commissioner for Patents, Washington, DC 20231 by "Express Mail Post Office to Addressee" service.

Lucretia Husain Lucretia Husain
Name (Print) Signature

APPLICATION
FOR
UNITED STATES LETTERS PATENT

TO ALL WHOM IT MAY CONCERN:

Be it known that Tal Lavian, Franco Travostino, Thomas Hardjono and Robert Duncan have invented a SECURITY ASSOCIATION MEDIATOR FOR JAVA-ENABLED DEVICES of which the following description in connection with the accompanying drawings is a specification, like reference characters on the drawings indicating like parts in the several Figures.

SECURITY ASSOCIATION MEDIATOR FOR JAVA-ENABLED DEVICES

FIELD OF THE INVENTION

This invention relates generally to the field of networking and more particularly to methods and apparatus for transferring files between devices in a secure manner.

BACKGROUND OF THE INVENTION

Data networks have become an essential part of most businesses. With the advent and wide acceptance of the Internet they have become even more essential.

Many network systems, such as telephone network products, data network products, etc. include externally developed software applications that call various functions within the network. It is desirable, however, to limit the functions and/or information that can be called by the application or the visitor to those that are necessary and/or approved.

It is thus important for a business to take precautions against downloading a code which may be potentially damaging to its network (e.g. a code which accesses the internal resources of a switch or router, such as the routing tables or filtering information, etc) and to take precautions against unauthorized access by outsiders.

It is unlikely that computers which access the Internet will ever be completely safe from attack from hackers and viruses. However, systems are available which provide a level of protection and security against such problems.

The Java environment includes security devices such as a security manager, a byte code verifier and a class loader. A security manager is a local device which determines whether potentially threatening or unauthorized operations should be allowed. A byte code verifier verifies the byte code transmitted with the download, and the class loader loads the Java Byte code to the JVM.

However, the security devices of a respective environment may not be backward compatible with earlier versions. In the Java environment, as an example, the security devices in version 1.2 are not backward compatible with those in versions 1.1 and 1.0.2, and the security devices in version 1.1 are not backwards compatible with those in version 1.0.2. Thus, an application program written in a respective version of Java is not compatible with other versions.

Furthermore, in some programming environments, such as in the Java environment, the security devices provide multi-level security but are not transparent, namely the user code must explicitly interact with the system, and the security devices are not dynamic, namely that off-line changes to the system may be necessary. Alternatively, the security devices are code transparent but do not provide multi-level security.

Accordingly, there exists a need for a security system which is system wide which prevents harmful programs from being downloaded onto a network.

There exists a need for a security system which is system wide and which prevents unauthorized access to the internal resources of a switch or router.

There also exists a need for such a system which enables a system view or configuration.

There also exists the need for such a system which is distributed.

There exists a need for such a system which allows other security entities to participate in the security system.

Accordingly, it is an object of the present invention to provide a security system which prevents harmful programs from being downloaded onto a network.

It is an object of the invention to provide a security system which prevents unauthorized access to the internal resources of a switch or router.

It is another object of the invention to provide such a system which is system wide and which enables a system view or configuration.

It is still another object of the invention to provide such a system which is distributed.

It is another object of the invention to provide a such a system which allows other security entities to participate in the security.

These and other objects of the invention will become apparent to those skilled in the art from the following description thereof.

SUMMARY OF THE INVENTION

In accordance with the teachings of the present invention, these and other objects may be accomplished by the present invention, which provides a method for providing security against unauthorized access to internal resources of a network device. The method includes receiving a digital signature at a security association manager (SAM) wherein the digital

signature includes an encryption code. The SAM requests a de-encryption code, de-encrypts the digital signature with the de-encryption code, authenticates the de-encrypted digital signature, and requests allowed operations associated with the authenticated signature.

An embodiment of the invention includes apparatus for providing security against unauthorized access to internal resources of a network device. The apparatus includes a security association manager (SAM) configured to receive a digital signature including an encryption code. The SAM is configured to send a message including a portion of the digital signature. The message includes a request for an encryption decoder. The SAM is further configured to receive a response to the message. The SAM is also configured to send a digitally signed message requesting allowed operations associated with the digital signature in response to receiving the reply message.

Another embodiment of the invention includes apparatus for providing security against unauthorized access to internal resources of a network device. The apparatus includes a module for receiving a digital signature including an encryption code. It also includes a module for accessing a de-encryption code in electrical communication with the module for receiving; and, it includes a module for determining allowed operations associated with the digital signature.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be more clearly understood by reference to the following detailed description of an exemplary embodiment in conjunction with the accompanying drawings, in which:

FIG. 1 illustrates a block diagram of a security system in accordance with the present invention.

FIG. 2 illustrates a block diagram of a distributed security system in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The invention provides a system and method of providing network security while transferring Java code between devices and/or while allowing access to Java enabled devices (e.g., within a network, between devices on a network and the Internet, between devices on separate networks, between network devices and application servers, and/or between network devices and databases.).

As illustrated in Fig. 1, the system provides a Security Association Manager 20 (SAM) which performs, *inter alia*, certain security tasks which are not performed by conventional Java security systems. The SAM 20 is distributed throughout the network and may be part of the class loader 10. Those skilled in the art will recognize that the SAM 20 may be integral with the class loader 10, co-located with, but logically separate from the class loader 10 or entirely distinct therefrom and still fall within the scope of the invention. The SAM 20 may be realized in hardware and/or software. As illustrated in Fig. 1,the system includes conventional class loaders 10, SAMs 20, a certificate authority 30, a policy server 40, access managers 50, security managers 70 and byte code verifier 60. The SAM 20 verifies the authenticity of the entity and either allows a download/access to a device or rejects the download/access to a network device. The certificate authority 30 is a repository for public key certificates and may be a part of the secure network or part of the unsecured network. The policy server 40 is a repository for the rights (privileges) an entity is entitled to on the secure network. The class loader 10 loads the Java Byte Code to the JVM. The Access Manager 50 assigns access levels to each Java thread that is created. The security manager 70 is a conventional security manager and the byte code verifier 60 verifies that the Byte code is valid Java code.

When Java code is to be transferred to a Java enabled network device (JEND) in the secure network, the code is digitally signed. A digital signature is generally a string of bits that is computed from a combination of the data being signed and a private key of an entity. A private key certificate (private key) is generally a number that is supposed to be known only to a particular entity, although it may not even be known to the entity (e.g. it may be associated with that entity through a program that entity employs). Either way, a private key is meant to be kept secret. A private key is always associated with a public key.

A digitally signed Java code is received by the class loader 10 and may be employed by the SAM 20, which is in communication with the class loader 10, to verify that the data came from an authorized entity or with the authority of an authorized entity. A digital signature can be authenticated via a computation that uses the public key corresponding to the private key used to generate the signature. It cannot be forged, assuming the private key is kept secret. It is a function of the data signed and thus can not be claimed to be the signature for other data as well. Further, the signed data cannot be changed; if it is, the signature will no longer authenticate.

The SAM 20 receives the digital signature, reads a name or code which is attached thereto then sends a request (including the name/code which was attached to the digital signature) for the public key certificate to the certificate authority 30. The certificate authority 30 compares the received request to the information stored therein. If no match is found then the certificate authority 30 responds to the SAM 20 with a message indicating failure (e.g., certificate does not exist, etc.). If the certificate authority finds a match, then it returns the public key certificate to the SAM 20.

If the SAM receives the failure notification it rejects the download/denies access. If the SAM receives the public key certificate, it authenticates the digital signature using the public key.

After the SAM 20 authenticates the digital signature, it sends a request for the rights the entity has on the secure network. The request is digitally signed or encrypted and sent to the policy server 40. While in the preferred embodiment the request to the policy server is digitally signed, it is possible to use other forms of security or no security at all if so desired, since the request typically will occur over the secure network and all SAMs could have the same rights to see the requested information. In the preferred embodiment the request is encoded since generally not all SAMs have the same rights on the network. The policy server 40 verifies the authenticity of the request from the SAM 20, then returns the access level stored in the policy server 40 corresponding to the request. The response is also digitally signed or encrypted to prevent it from being modified during transit. However, since this is also traveling over the secured network it is foreseeable that this message could be designed to have no security attached to it. Once the SAM receives this information and authenticates

the transmission, it allows the download of the code/access to the system to take place within the limits of the entity's rights on the network.

The operation of the SAM with respect to providing further access is described in further detail in U.S. Application Serial No. _____, filed concurrently herewith (NTL-3.2.077/2128), which is incorporated herein by reference.

It will thus be seen that the invention efficiently attains the objects set forth above, among those made apparent from the preceding description. In particular, the invention provides methods and apparatus for providing network security against unauthorized access to Java enabled devices. Those skilled in the art will appreciate that the configuration depicted in Figures 1 and 2 provide such features.

It will be understood that changes may be made in the above construction and in the foregoing sequences of operation without departing from the scope of the invention. It is accordingly intended that all matter contained in the above description or shown in the accompanying drawings be interpreted as illustrative rather than in a limiting sense.

It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention as described herein, and all statements of the scope of the invention which, as a matter of language, might be said to fall there between.

Having described the invention, what is claimed as new and secured by Letters Patent is: